Nationale Strategie zum Schutz kritischer Infrastrukturen

vom 27. Juni 2012

Zusammenfassung

Kritische Infrastrukturen stellen die Verfügbarkeit von essenziellen Gütern und Dienstleistungen, wie etwa Energie, Kommunikation oder Verkehr, sicher. Grossflächige Ausfälle wirken sich schwerwiegend auf die Bevölkerung und die Wirtschaft aus. Ebenso beeinträchtigen sie die Sicherheit und das Wohlergehen des Staates.

Die Schweiz verfügt in einzelnen Bereichen bislang über ein hohes Schutzniveau und profitiert von einem relativ stabilen Umfeld, sodass schwerwiegende Ausfälle bisher selten und von kurzer Dauer waren. Die Bedeutung der kritischen Infrastrukturen hat aber im Zuge der Technologisierung und der Globalisierung stark zugenommen: Ein landesweiter Blackout in der Stromversorgung würde beispielsweise die gesamte Volkswirtschaft lahmlegen, zu Ausfällen der übrigen kritischen Infrastrukturen (z.B. der Telekommunikation, der Wasserversorgung oder des Schienenverkehrs) führen und die Bevölkerung in schwerwiegendem Masse beeinträchtigen (Ausfall von Beleuchtungen, (Tief-)Kühlanlagen, Heizungen, Aufzügen usw.). Ebenfalls haben sich in letzter Zeit die Risiken verändert, etwa durch zunehmende Naturkatastrophen, Cyber-Angriffe oder die Überalterung von technischen Systemen. Weiter verlangen die starken gegenseitigen Abhängigkeiten im Ereignisfall (Interdependenzen) nach einer verstärkten Zusammenarbeit aller Akteure über die verschiedenen Sektoren der kritischen Infrastrukturen hinweg.

Aus diesen Gründen ist es notwendig, mit der vorliegenden nationalen Strategie die Resilienz (Widerstandsfähigkeit) der Schweiz im Zusammenhang mit kritischen Infrastrukturen in umfassender Weise zu verstärken. Die Strategie bezeichnet dazu verschiedene Massnahmen in zwei Bereichen (Handlungsfeldern). Im Bereich der kritischen Infrastrukturen *wird der Selbstschutz verbessert, indem die zuständigen Stellen integrale Schutzkonzepte erarbeiten und umsetzen. Darin werden infrastrukturspezifische Risiken identifiziert und reduziert. Im* Infrastruktur-übergreifenden Bereich *werden die Zusammenarbeit der Akteure (Behörden, Betreiber) aus den verschiedenen Sektoren der kritischen Infrastrukturen verbessert und die Verletzlichkeit von Gesellschaft, Wirtschaft und Staat gegenüber schwerwiegenden Ausfällen verringert. Zu diesem Zweck werden Planungen zur Schadensbewältigung bei schwerwiegenden Ausfällen und zur subsidiären Unterstützung der Betreiber bei solchen Ereignissen erarbeitet. Weitere Massnahmen betreffen die Gewährleistung einer zeitgerechten Warnung im Ereignisfall oder die Stärkung der Selbstvorsorge bei der Bevölkerung und der Wirtschaft im Hinblick auf schwerwiegende Ausfälle.*

Im Umfeld des Schutzes kritischer Infrastrukturen sind verschiedene Vorhaben, Massnahmen, Projekte usw. von Bedeutung. Dementsprechend erfolgt auch die Umsetzung der nationalen Strategie zum Schutz kritischer Infrastrukturen massgeblich im Rahmen der bestehenden Strukturen und Zuständigkeiten. Die Kompetenzen der beteiligten Bundesstellen bleiben vorbehalten.

Nationale Strategie

1 Einleitung

Die Schweiz ist in grossem Masse auf ein möglichst kontinuierliches Funktionieren von kritischen Infrastrukturen (KI) angewiesen. Diese stellen die Verfügbarkeit von wichtigen Gütern und Dienstleistungen wie Energie, Kommunikation oder Verkehr sicher. Ausfälle von kritischen Infrastrukturen haben schwerwiegende Auswirkungen auf die Wirtschaft und die Bevölkerung und beeinträchtigen die Sicherheit und das Wohlergehen des Staates. Der Schutz kritischer Infrastrukturen (SKI) ist deshalb eine zentrale Aufgabe des staatlichen und betrieblichen Handelns.

Der Schutz von kritischen Infrastrukturen ist an sich nichts Neues. In einzelnen Bereichen der kritischen Infrastrukturen oder im Hinblick auf spezifische Gefährdungen oder Gegenmassnahmen beschäftigen sich die jeweils zuständigen Stellen auf den Ebenen Bund, Kantone und Betreiber mit Aspekten, die zum übergeordneten Ziel beitragen. Gefehlt haben aber lange Zeit eine übergreifende Koordination sowie ein abgestimmtes und umfassendes Vorgehen in den verschiedenen Bereichen.

Der Bundesrat hat das Bundesamt für Bevölkerungsschutz (BABS) mit der Koordination der Arbeiten im SKI-Bereich und der Erarbeitung einer nationalen SKI-Strategie bis im Frühjahr 2012 beauftragt.

Die nationale SKI-Strategie hält fest, welche Ziele die Schweiz im SKI-Bereich verfolgt und zeigt auf, welche Massnahmen getroffen werden, um Risiken im Zusammenhang mit kritischen Infrastrukturen zu reduzieren. Damit trägt die Strategie massgeblich zum Schutz der Bevölkerung, zur Erhaltung des wirtschaftlichen Wohlstands und zur Sicherheit des Landes bei.

Die Strategie umschreibt den Geltungsbereich, bezeichnet die kritischen Infrastrukturen und hält die übergeordneten Grundsätze beim Schutz kritischer Infrastrukturen fest. Weiter gibt sie einen Überblick über den aktuellen Stand der SKI-Arbeiten in der Schweiz und im Ausland. Sie hält die Vision und die Ziele fest und nennt 15 Massnahmen, die zwei Handlungsfeldern zugewiesen werden. Zum Schluss zeigt sie auf, in welchen Strukturen und mit welchen Zuständigkeiten die SKI-Strategie umgesetzt wird.

Die nationale SKI-Strategie richtet sich an alle Stellen, die im Umfeld des Schutzes kritischer Infrastrukturen Verantwortlichkeiten aufweisen, insbesondere an die jeweils zuständigen Behörden (Bund, Kantone und Gemeinden), die politischen Entscheidungsträger und die Betreiber von kritischen Infrastrukturen.

2 Geltungsbereich und Bezeichnung der kritischen Infrastrukturen

Der Geltungsbereich der nationalen Strategie zum Schutz kritischer Infrastrukturen wird durch die Definition der relevanten Begriffe sowie die Bezeichnung und Einteilung der kritischen Infrastrukturen abgegrenzt.

Infrastrukturen

Der Sammelbegriff «Infrastrukturen» umfasst Einrichtungen und Organisationen, die Dienstleistungen und Produkte für die Gesellschaft, die Wirtschaft und den Staat liefern

Kritische Infrastrukturen

Kritische Infrastrukturen sind Infrastrukturen, deren Störung, Ausfall oder Zerstörung gravierende Auswirkungen auf die Gesellschaft, die Wirtschaft und den Staat hat. Die kritischen Infrastrukturen werden in drei Ebenen unterteilt:

- *Sektoren:* z.B. Energie, Finanzen, Gesundheit
- *Teilsektoren:* z.B. Stromversorgung, Erdölversorgung, Erdgasversorgung
- *(Einzel-)Objekte/Elemente:* z.B. Leitstellen, Steuerungssysteme, Rechenzentren, Stauanlagen, Rohrleitungen, Betreiberfirmen

Das Spektrum der kritischen Infrastrukturen gestaltet sich wie folgt:

Tabelle 1

Liste der kritischen Infrastrukturen

Sektoren	Teilsektoren
Behörden	Diplomatische Vertretungen und Sitze internationaler Organisationen
	Forschung und Lehre
	Kulturgüter
	Parlament, Regierung, Justiz, Verwaltung
Energie	Erdgasversorgung
	Erdölversorgung
	Stromversorgung
Entsorgung	Abfälle
	Abwasser
Finanzen	Banken
	Versicherungen
Gesundheit	Ärztliche Betreuung und Spitäler
	Labors
Industrie	Chemie- und Heilmittelindustrie
	Maschinen-, Elektro- und Metallindustrie
Information und Kommunikation	Informationstechnologien
	Medien
	Postverkehr
	Telekommunikation
Nahrung	Lebensmittelversorgung
	Wasserversorgung
Öffentliche Sicherheit	Armee
	Blaulichtorganisationen (Polizei, Feuerwehr, Sanität)
	Zivilschutz
Verkehr	Luftverkehr
	Schienenverkehr
	Schiffsverkehr
	Strassenverkehr

	Sehr grosse Kritikalität*
	Grosse Kritikalität*
	Reguläre Kritikalität*

* – Die Kritikalität steht für die relative Bedeutung des Teilsektors bezüglich Bevölkerung, Wirtschaft und Dependenzen (≠ absolute Bedeutung). Zur Ableitung eines allfälligen Handlungsbedarfs sind zusätzlich jeweils die konkrete Bedrohungslage und die Verletzlichkeit der kritischen Infrastrukturen zu berücksichtigen.
– Die Gewichtung macht keine Aussagen über die Kritikalität von Einzelobjekten.
– Die Gewichtung orientiert sich an einer normalen Gefährdungslage.

Schutz kritischer Infrastrukturen

Der Schutz kritischer Infrastrukturen umfasst Massnahmen, die die Eintrittswahrscheinlichkeit und/oder das Schadenausmass einer Störung, eines Ausfalls oder einer Zerstörung von kritischen Infrastrukturen reduzieren beziehungsweise die Ausfallzeit minimieren.

3 Grundsätze für den Schutz kritischer Infrastrukturen

Umfassender, risikobasierter Ansatz: Der Schutz kritischer Infrastrukturen erfolgt risikobasiert. Das Risiko ergibt sich aus der Gefährdung, der Kritikalität und der Verletzlichkeit. Die Gefährdungsanalyse berücksichtigt dabei ein umfassendes Gefahrenspektrum. Dies bedeutet, dass prinzipiell jede relevante Gefahr (Naturgefahren, technische Gefahren, gesellschaftliche Gefahren)[1] berücksichtigt wird. Auch bei den zu evaluierenden Schutzmassnahmen ist ein umfassendes Massnahmenspektrum zu berücksichtigen (bauliche, technische, organisatorische und rechtliche Aspekte in den Phasen Prävention, Vorsorge, Notfall- und Krisenbewältigung, Instandstellung und Wiederaufbau). Dabei ist auch der Schutz der Informationen sicherzustellen.

Verhältnismässigkeit: Bei den Massnahmen zum Schutz kritischer Infrastrukturen sind die Kosten zur Umsetzung mit dem Nutzen ins Verhältnis zu setzen. Die gewählten Massnahmen müssen überdies verfassungskonform und rechtlich legitimiert sein. Es darf zudem nicht zu unnötigen Marktverzerrungen kommen.

Selbstverantwortung: Massnahmen müssen sowohl von öffentlicher Seite als auch von Seiten der KI-Betreiber ergriffen werden. Da ein grosser Teil der kritischen Infrastrukturen von privaten Unternehmen betrieben wird, ist die eigenständige Verbesserung der Schutzmassnahmen von grosser Bedeutung. Die jeweils zuständigen Behörden sind aufgefordert zu überprüfen, ob dies ausreichend; gegebenenfalls sollen sie entsprechende Schutz- und Leistungsziele auf politischer Ebene festlegen.

Öffentlich-private Zusammenarbeit (public private partnership): Der Schutz kritischer Infrastrukturen verlangt eine verstärkte Zusammenarbeit zwischen allen involvierten Akteuren (Behörden auf den Ebenen Bund, Kantone und Gemeinden sowie Betreiber). Wo möglich, sollen Schutzmassnahmen gemeinsam erarbeitet und umgesetzt werden. Die öffentlich-private Zusammenarbeit ist in allen Bereichen des Schutzes kritischer Infrastrukturen zu prüfen, insbesondere bei baulichen Vorhaben (z.B. bei Neubauten von kritischen Infrastrukturen), bei der Erarbeitung von Richtlinien und Normen oder bezüglich des Informationsaustauschs.

1 Die Einteilung der Gefährdungen orientiert sich an den Arbeiten zu «Risiken Schweiz».

4 Aktueller Stand Schutz kritischer Infrastrukturen

4.1 Schutz kritischer Infrastrukturen in der Schweiz

Folgende Situation präsentiert sich im Hinblick auf die Thematik Schutz kritischer Infrastrukturen in der Schweiz:

- Es besteht bereits eine Vielzahl von Organisationen, Strukturen, Massnahmen, Regelungen, Projekten usw., die zum Schutz der kritischen Infrastrukturen beitragen.[2] Vielfach sind diese Arbeiten in spezifische Politikbereiche eingebettet, etwa in die Energiepolitik, die Verkehrspolitik oder die Sicherheitspolitik. Die Arbeiten beschränken sich dabei meist auf einzelne Sektoren, einzelne Gefährdungen oder spezifische Gegenmassnahmen. Zudem werden in der Regel unterschiedliche methodische Ansätze, etwa zur Bewertung von Gefährdungen und zur Ableitung von Gegenmassnahmen, verfolgt.
- Aspekte des Schutzes sind in den Politikbereichen der kritischen Teilsektoren indes vielfach von eher untergeordneter Wichtigkeit, und es fehlt eine explizite und umfassende Berücksichtigung der Thematik. Die Bedeutung der kritischen Infrastrukturen nimmt jedoch u.a. infolge der Technologisierung ständig zu, und die Schweiz ist in immer grösserem Masse auf ihr kontinuierliches Funktionieren angewiesen. Grossflächige Ausfälle beispielsweise der Stromversorgung oder der Telekommunikation würden heute ungleich schwerwiegendere Auswirkungen verursachen, als dies noch vor einigen Jahren der Fall war. Verändert haben sich auch die Gefährdungen, die zu solchen Ausfällen führen können (Cyber-Bedrohung, Terrorismus, zunehmende Naturgefahren usw.). Schliesslich hat auch die Verletzlichkeit zugenommen, unter anderem weil die kritischen Infrastrukturen vielfach grenzüberschreitende Systeme darstellen, in denen kleine Störungen bereits Konsequenzen auf internationaler Ebene verursachen können. Zudem wurden Produktions- und Verteilprozesse vielerorts automatisiert und Redundanzen wurden abgebaut.
- Im Juni 2009 hat der Bundesrat die Grundstrategie zum Schutz kritischer Infrastrukturen verabschiedet.[3] Mit dieser konnten zwar die Koordination und die Grundlagen im SKI-Bereich verbessert werden, das systematische und umfassende Vorgehen ist jedoch noch nicht in allen Bereichen vollumfänglich etabliert.

2 Im Teilsektor Stromversorgung erarbeitet der Bund beispielsweise u.a. eine Strategie Energienetze, welche zum Ziel hat, auch weiterhin ein sicheres und leistungsfähiges Stromnetz zu gewährleisten. Zudem befasst sich das Programm zur Erdbebenvorsorge mit der Härtung der Strominfrastruktur gegenüber Erdbeben. Weiter erarbeitet die wirtschaftliche Landesversorgung Planungen zur Strombewirtschaftung im Krisenfall, welche von der Organisation für die Stromversorgung in ausserordentlichen Lagen (OSTRAL) vollzogen werden.

3 Die «Grundstrategie zum Schutz Kritischer Infrastrukturen» ist unter folgender Internetadresse abrufbar: www.bevoelkerungsschutz.admin.ch > Themen > Schutz Kritischer Infrastrukturen

4.2 SKI-Strategien im Ausland

Verschiedene Staaten haben in den letzten Jahren nationale Strategien zum Thema Schutz kritischer Infrastrukturen verabschiedet respektive aktualisiert. Ein Vergleich verschiedener Strategien zeigt, dass folgende Aspekte im Zentrum stehen:

- Förderung des Dialogs und der Zusammenarbeit (sektorspezifisch und sektorübergreifend), indem so genannte Plattformen (Deutschland) oder «Secretariats» (USA, Australien) gebildet werden. Darin sind jeweils die Behörden und die KI-Betreiber vertreten.
- Erstellen eines Verzeichnisses von kritischen Infrastrukturen, respektive Identifikation von einzelnen kritischen Objekten (u.a. Frankreich und Deutschland). Teilweise werden die kritischen Infrastrukturen allerdings nur generisch bezeichnet (z.B. Kraftwerk), ohne weiter zu bestimmen, um welche konkreten Objekte es sich handelt. Auch die Europäische Union erstellt derzeit in den Sektoren Energie und Verkehr ein Verzeichnis der europäisch kritischen Infrastrukturen, wobei der Fokus auf den grenzüberschreitenden Auswirkungen von Infrastrukturausfällen liegt.
- Erarbeitung von Schutzkonzepten und -plänen für die als kritisch identifizierten Infrastrukturen; dies geschieht in der Regel nach einem in der Strategie vorgegebenen Rahmenprozess (insbesondere USA).

Der Vergleich zeigt weiter, dass in keiner der untersuchten Strategien konkrete Aussagen zu Defiziten in einzelnen Sektoren der kritischen Infrastrukturen, zu einzelnen Gegenmassnahmen oder zu Folgekosten von allfälligen Massnahmen gemacht werden. Stattdessen steht jeweils die Sicherstellung eines einheitlichen und umfassenden Vorgehens im Vordergrund.

5 Vision und Ziele der nationalen SKI-Strategie

5.1 Vision

Mit der nationalen SKI-Strategie soll folgende Vision verfolgt werden:

«Die Schweiz ist im Hinblick auf die Funktionsfähigkeit der kritischen Infrastrukturen resilient, sodass grossflächige und schwerwiegende Ausfälle der kritischen Infrastrukturen und der damit verbundenen Güter und Dienstleistungen möglichst verhindert werden beziehungsweise das Schadenausmass im Ereignisfall begrenzt bleibt.»

5.2 Ziele

Die nationale SKI-Strategie hat zum Ziel, die Resilienz der Schweiz in Bezug auf kritische Infrastrukturen zu stärken. Sie soll zudem ein koordiniertes Vorgehen aller Akteure gewährleisten.

Die Resilienz bezieht sich auf die Fähigkeit eines Systems, einer Organisation oder einer Gesellschaft, intern oder extern verursachten Störungen zu widerstehen und die Funktionsfähigkeit möglichst zu erhalten, respektive wieder zu erlangen. Die Resilienz setzt sich aus vier Bestandteilen zusammen:

1. der Robustheit der Systeme (kritische Infrastrukturen, Staat, Wirtschaft und Gesellschaft) an sich;
2. der Verfügbarkeit von Redundanzen;
3. der Fähigkeit, wirksame Hilfsmassnahmen zu mobilisieren;
4. der Schnelligkeit und Effizienz der Hilfsmassnahmen.

Gestützt auf diese Ausführungen werden die Ziele der nationalen SKI-Strategie in zwei Bereiche unterteilt. Die nationale SKI-Strategie soll demnach:

– die Robustheit und Flexibilität der kritischen Infrastrukturen stärken;
– im KI-übergreifenden Bereich die Zusammenarbeit verbessern, die Robustheit und Flexibilität von Gesellschaft, Wirtschaft und Staat (Bund, Kantone und Gemeinden) stärken und sicherstellen, dass im Hinblick auf einen Ereignisfall effektive und schnelle Hilfsmassnahmen und Redundanzen bereitstehen.

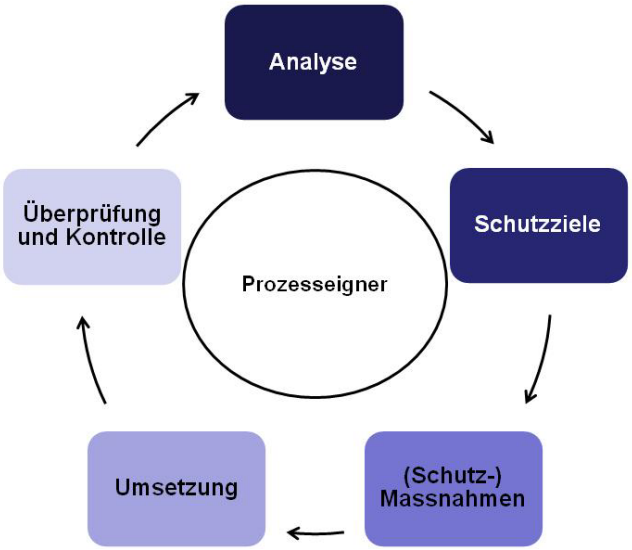
Die Ziele sollen erreicht werden, indem mit Hilfe eines abgestimmten und koordinierten Vorgehens in diesen beiden Bereichen jeweils der *integrale Schutz* (vgl. Kap. 6) verbessert wird.

6 Integraler Schutz

Der integrale Schutz beruht auf einem systematischen Prozess, der von einem jeweils zuständigen Prozesseigner geführt wird (diese werden in Ziff. 8 bezeichnet).

Abbildung 1

Integraler Schutzprozess



Dabei sind jeweils folgende Ziele zu erreichen:

Analyse

- Kritische Prozesse, Systeme, Objekte usw. sind identifiziert und priorisiert.
- Risiken und Verletzlichkeiten, die zu schwerwiegenden Ausfällen führen können, sind identifiziert und bewertet.
- Relevante Änderungen der Bedrohungslage im Zusammenhang mit kritischen Infrastrukturen sind zeitgerecht erkannt.

Schutzziele

- Schutz- und Leistungsziele sind auf politischer Ebene festgelegt und auf die betriebliche Ebene transformiert.

(Schutz-)Massnahmen

- Gestützt auf die vereinbarten Schutz- und Leistungsziele sind durch die jeweils zuständigen Stellen Massnahmen (inkl. Konzepte, Strukturen, Prozesse und Instrumente) bezeichnet, mit denen:
  - grossflächige und schwerwiegende Ausfälle möglichst verhindert werden,
  - Bedrohungen abgewehrt und Ereignisse bewältigt werden können, und
  - eine rasche Rückkehr zum Normalbetrieb ermöglicht wird.

  Die Massnahmen orientieren sich dabei an einem risikobasierten Kosten-Wirksamkeits-Ansatz.

Umsetzung

- Die definierten Massnahmen sind umgesetzt.

Überprüfung und Kontrolle

- Die Wirkung der getroffenen Massnahmen ist überprüft.
- Massnahmen sind mit Hilfe von Übungen gefestigt.

7 Massnahmen der nationalen SKI-Strategie

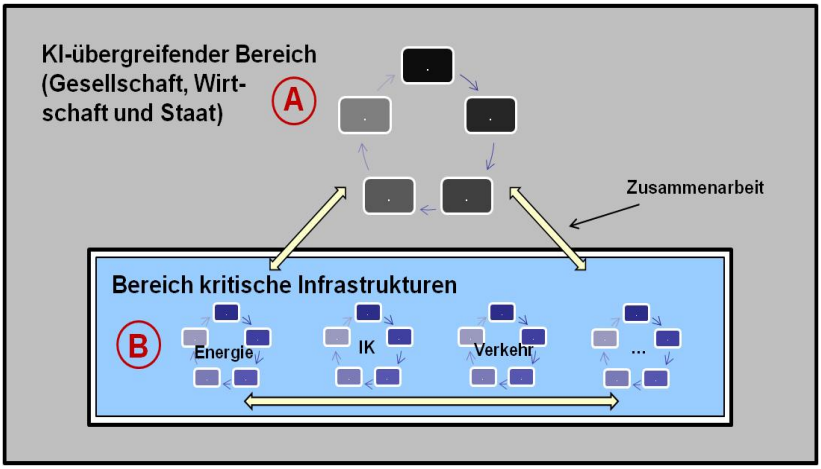
In Anlehnung an die Ziele (vgl. Ziff. 5) nennt die nationale SKI-Strategie Massnahmen, die den *integralen Schutz* jeweils in zwei Bereichen (Handlungsfeldern) stärken:

- Im *KI-übergreifenden Bereich* sollen das koordinierte Vorgehen sichergestellt und die Robustheit von Gesellschaft, Wirtschaft und Staat gegenüber Ausfällen der kritischen Infrastrukturen verbessert werden *(Handlungsfeld A)*. Dazu werden Prozesse etabliert, die mehrere kritische Infrastrukturen betreffen (u.a. zur Verbesserung der Koordination und zur Unterstützung der Betreiber mit Hilfsmitteln im Ereignisfall) und Massnahmen zur Verringerung der Verletzlichkeit von Gesellschaft, Wirtschaft und Staat gegenüber Ausfällen kritischer Infrastrukturen getroffen;

– Im *Bereich der kritischen Infrastrukturen*, soll der Selbstschutz respektive die Robustheit der kritischen Infrastrukturen verbessert werden *(Handlungsfeld B)*. Dazu werden infrastrukturspezifische Risiken identifiziert und reduziert. Indem der Selbstschutz der verschiedenen kritischen Infrastrukturen verbessert wird und ein einheitliches Vorgehen die Kompatibilität der Massnahmen gewährleistet, lassen sich unter anderem auch die Risiken der wechselseitigen Abhängigkeiten (Interdependenzen) reduzieren.

Abbildung 2

Handlungsfelder der nationalen SKI-Strategie



Nachfolgend werden in diesen beiden Handlungsfeldern jeweils Massnahmen bezeichnet, die zur Erreichung der in den vorangegangenen Ziffern beschriebenen Ziele beitragen.

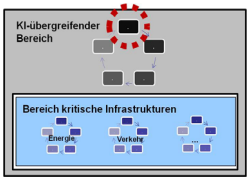
Wie in Ziffer 4.1 festgehalten, sind im Zusammenhang mit dem Schutz kritischer Infrastrukturen verschiedene bereits etablierte oder geplante Projekte, Vorhaben, Massnahmen usw. relevant. Vielfach wird es bei der Umsetzung der nationalen SKI-Strategie deshalb darum gehen, bestehende Prozesse zu überprüfen und gegebenenfalls zu ergänzen. Wo immer möglich, baut die nationale SKI-Strategie auf Bestehendem auf. Im Detail wird der Abgleich im Rahmen der Umsetzungsplanung sichergestellt. Im Anhang wird ein Überblick über die Massnahmen und die wichtigsten Nahtstellen mit anderen Arbeiten gegeben; im Text wird auf eine explizite Nennung verzichtet.

7.1 Integralen Schutz im KI-übergreifenden Bereich stärken (Handlungsfeld A)

Der integrale Schutz im KI-übergreifenden Bereich umfasst alle Tätigkeiten, die für die Gestaltung, Steuerung und Weiterentwicklung der SKI-relevanten Aktivitäten erforderlich sind. Er soll die Resilienz von Staat, Wirtschaft und Gesellschaft erhöhen und die notwendigen Rahmenbedingungen für SKI schaffen. Die Massnahmen orientieren sich dabei am integralen Schutz gemäss Ziffer 6, wobei die Phasen «Umsetzung» sowie «Überprüfung und Kontrolle» in Ziffer 8 der Strategie behandelt werden.

Analyse

Kritische Infrastrukturen identifizieren und priorisieren



Bevor Schutzmassnahmen getroffen werden können, müssen die zuständigen Stellen wissen, welche Infrastrukturen besonders kritisch sind. Kenntnisse über die kritischen Infrastrukturen und ihre Bedeutung sind auch notwendig, um im Falle von Ereignissen Lagebeurteilungen vornehmen zu können.

In diesem Zusammenhang wird gestützt auf die SKI-Grundstrategie des Bundesrates das Inventar kritischer Infrastrukturen erarbeitet (SKI-Inventar). Dabei werden sowohl Einzelobjekte (Bauten und Anlagen) identifiziert, die auf nationaler Ebene kritisch sind, als auch durch die Kantone diejenigen, die auf kantonaler oder lokaler Ebene kritisch sind. Nach Möglichkeit wird dazu auf Daten zurückgegriffen, die bereits im Rahmen von anderen Verzeichnissen erfasst wurden.

Ziel:

– Die kritischen Infrastrukturen der Schweiz sind identifiziert und unter Wahrung der Informationsschutzvorschriften (bei klassifizierten Informationen) mit aktualisierten Angaben erfasst. Insbesondere sind kritische Systeme und Objekte erkannt und priorisiert.

Massnahme:

– *M1:* Es ist ein periodisch aktualisiertes Verzeichnis der kritischen Infrastrukturen der Schweiz zu führen (SKI-Inventar), sodass unter Wahrung des Informationsschutzes für verschiedene Bedürfnisträger zeitgerecht Auszüge erstellt werden können. Dabei ist zu prüfen, wie unter Wahrung der rechtlichen Grundlagen auf bestehende Objektverzeichnisse zurückgegriffen werden kann.

Risiken, Verletzlichkeiten und Schutzmöglichkeiten kennen

Als Grundlage für die Verbesserung des integralen Schutzes der kritischen Infrastrukturen müssen sektorübergreifende Aussagen über relevante Risiken gemacht werden können. Dazu benötigt es insbesondere einen Katalog der zu berücksichtigenden Risiken sowie Aussagen zur Eintrittswahrscheinlichkeit und zum Schadenausmass dieser Risiken. Diese Gefährdungsannahmen werden auf Ebene der kritischen Infrastrukturen mit konkreten Risikobetrachtungen ergänzt.

Zudem sind zur methodischen Weiterentwicklung des Schutzes kritischer Infrastrukturen wissenschaftlich fundierte Erkenntnisse, etwa in den Bereichen der Interdependenz- oder Kritikalitätsanalysen, notwendig. Ferner müssen Technologieentwicklungen oder Umwelt- und Umfeldentwicklungen verfolgt werden, die zu neuen Risiken führen können.

Ziele:

- Eine periodisch aktualisierte Übersicht über die relevanten Gefährdungen mit einer Einschätzung ihrer Eintrittswahrscheinlichkeit und ihres Schadenausmasses liegen vor.
- Es sind wissenschaftlich fundierte Grundlagen vorhanden, die zur methodischen Weiterentwicklung des integralen Schutzes beitragen.

Massnahme:

- *M2:* Es sind Forschungsprogramme (z.B. nationales Forschungsprogramm) im Hinblick auf methodische Grundlagen und sektorübergreifende Themen wie Interdependenz- und Kritikalitäts-Analysen, Resilienz-Metrik oder Technologie-Entwicklungen zu lancieren.

Zusammenarbeit und Informationsaustausch verbessern

Kritische Infrastrukturen sind hochgradig (inter-)dependent. Eine Zusammenarbeit und ein Dialog über Risiken und mögliche Schutzmassnahmen (*best practice*) zwischen den verschiedenen kritischen Infrastrukturen ist deshalb von zentraler Bedeutung. Die Zusammenarbeit soll dabei sowohl zwischen den Betreibern der kritischen Infrastrukturen als auch zwischen den zuständigen Behörden und Fachstellen verbessert werden. Da kritische Infrastrukturen vielfach grenzüberschreitende Systeme darstellen, ist auch die internationale Zusammenarbeit von Bedeutung.

Ziel:

- Unter Wahrung des Informationsschutzes (bei klassifizierten Informationen) besteht ein sektorübergreifender und institutionalisierter Informationsaustausch über Risiken, Verletzlichkeiten und mögliche Schutzmassnahmen (*best practice*).

Massnahme:

- *M3:* Es sind Plattformen zur Förderung der Zusammenarbeit zwischen den Fachstellen/Behörden aus den verschiedenen Bereichen des Schutzes kritischer Infrastrukturen (AG SKI), zwischen den Betreibern der kritischen Infrastrukturen (AG Betreiber) und mit den ausländischen Partnern im SKI-Bereich zu führen.

Warnung im Ereignisfall gewährleisten

Im Fall von akuten Bedrohungen ist eine rechtzeitige Warnung von grosser Bedeutung, um angemessene Gegenmassnahmen einleiten zu können. Dazu müssen einerseits relevante Änderungen der (kurzfristigen) Bedrohungslage erkannt werden. Für verschiedene Gefährdungen bestehen etablierte Verfahren, um solche Änderungen frühzeitig zu erkennen. Dies ist jedoch nicht für alle relevanten Gefährdungen in gleichem Masse gewährleistet (insbesondere nicht für technische Gefährdungen). Andererseits gilt es sicherzustellen, dass die Warnung frühzeitig und über fest defi-

nierte Schnittstellen erfolgt. Auch in diesem Zusammenhang gibt es bereits verschiedene etablierte Mechanismen. Diese verfügen aber zum Teil über nicht genügend (personelle) Ressourcen, oder es sind nicht alle Betreiber gemäss ihrer Bedeutung integriert. Gewisse Prozesse sind zudem nicht kanalisiert und berücksichtigen jeweils unterschiedliche Kontaktpersonen.

Ziele:

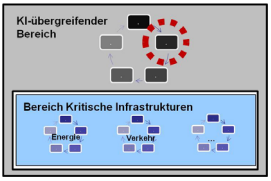
- Relevante Änderungen der (kurzfristigen) Bedrohungslage im umfassenden Gefahrenspektrum werden zeitgerecht erkannt.
- Betreiber kritischer Infrastrukturen werden gemäss ihrer Bedeutung frühzeitig und auch in Ausnahmesituationen in ausreichender Qualität vor akuten Bedrohungen gewarnt. Dabei ist gewährleistet, dass ein umfassendes Gefahrenspektrum abgedeckt wird, der Warnprozess mit Hilfe von gesicherten respektive geschützten Verbindungen über klar definierte Kontakte verläuft und der Informationsschutz gewahrt wird.

Massnahmen:

- *M4:* Befugnisse und Kapazitäten zur Erkennung und Überwachung von Gefährdungen und Gefahren sind im Hinblick auf alle Lagen zu überprüfen.
- *M5:* Es ist basierend auf den bestehenden Prozessen und Strukturen ein Mechanismus zu etablieren, der gewährleistet, dass alle relevanten Betreiber kritischer Infrastrukturen zeitgerecht über bedeutende Änderungen der Bedrohungslage gewarnt werden.

Schutzziele

Übergeordnete Schutzziele vorgeben



Die Schutzziele geben Auskunft über das angestrebte Schutz- und Leistungsniveau. Die Festlegung der Schutzziele erfolgt auf politisch-gesellschaftlicher Ebene. Es ist anzustreben, dass für die verschiedenen kritischen Infrastrukturen in einem politischen Prozess aufeinander abgestimmte und verbindliche Schutzziele vorgegeben werden. Aufgrund der Heterogenität der kritischen Infrastrukturen und der politischen Bedeutung der Thematik stellt dies ein äusserst schwieriges Unterfangen dar. Aus diesem Grund dient die in der Strategie beschriebene Vision als Schutzziel im KI-übergreifenden Bereich. Die Konkretisierung der Schutzziele erfolgt bei der Erarbeitung der integralen Schutzkonzepte im Bereich der kritischen Infrastrukturen (vgl. Massnahme M15). Nach Möglichkeit werden dafür Revisionen von bestehenden Rechtsgrundlagen genutzt. Bereits bestehende Schutzziele sind dabei zu berücksichtigen.

Ziel:

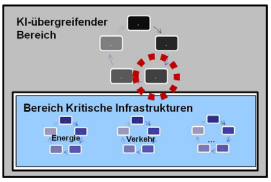
- Für die verschiedenen kritischen Infrastrukturen sind auf einander abgestimmte Schutzziele vorgegeben.

Massnahme:

- *M6:* Es sind auf einander abgestimmte Schutzziele zu erarbeiten und durch die Politik zu verabschieden.

(Schutz-)Massnahmen

Ausfälle von kritischen Infrastrukturen verhindern



Im KI-übergreifenden Bereich können verschiedene Massnahmen getroffen werden, um Risiken zu reduzieren, die für alle kritischen Infrastrukturen relevant sind, und um schwerwiegende Ausfälle von Kritischen Infrastrukturen zu verhindern. Solche generische Risiken betreffen etwa das Personal, das für die Durchführung von zentralen Prozessen verantwortlich ist. Um den hohen Sicherheitsstandards zu genügen und einen Austausch mit klassifizierten Informationen zu ermöglichen, sollten solche Personen einer Sicherheitsüberprüfung unterzogen werden können. Ein weiteres generisches Risiko stellt die Versorgung der kritischen Infrastrukturen mit Energie und Telekommunikation dar. Diesbezüglich stärken sie einerseits im Rahmen von Handlungsfeld B ihren Selbstschutz (vgl. Ziff. 7.2). Andererseits sollen national kritische Infrastrukturen im Rahmen von Priorisierungs- und Bewirtschaftungsplänen nach technischer Möglichkeit prioritär behandelt werden.

Ziele:

– Personen, die Zugang zu zentralen Prozessen[4] im Bereich der kritischen Infrastrukturen haben, sind sicherheitsüberprüft.

– National kritische Infrastrukturen werden bei Bewirtschaftungsmassnahmen oder Abschaltungen in den Bereichen Energie und Telekommunikation nach technischer Möglichkeit und nach Bedarf prioritär behandelt.

Massnahmen:

– *M7:* Es ist eine gesetzliche Grundlage zur Sicherheitsüberprüfung von ausgewähltem Personal der Betreiber kritischer Infrastrukturen zu schaffen.

– *M8:* Bestehende Abschalt- und/oder Bewirtschaftungspläne sind nach technischer Möglichkeit mit national kritischen Infrastrukturen zu ergänzen.

Vorsorge von Staat, Wirtschaft und Bevölkerung verbessern

Schwerwiegende Ausfälle von kritischen Infrastrukturen können das Funktionieren von Staat und Wirtschaft sowie die Bevölkerung in schwerwiegendem Masse beeinträchtigen. Das Schadenausmass kann reduziert werden, wenn Staat, Wirtschaft und Bevölkerung angemessen vorbereitet sind. Aus diesem Grund kommen vorsorglichen Planungen zur Bewältigung der Ereignisse und einer vorgängigen Sensibilisierung der Bevölkerung und der Wirtschaft über mögliche Risiken und selbstvorsorgliche Massnahmen grosse Bedeutung bei.

Ziel:

– Staat, Wirtschaft und Bevölkerung sind im Hinblick auf schwerwiegende Ausfälle von kritischen Infrastrukturen vorbereitet, so dass die Auswirkungen reduziert und Ereignisse bewältigt werden können.

4 Die Bezeichnung dieser Prozesse erfolgt bei der Erarbeitung des SKI-Inventars.

Massnahmen:

- *M9:* Bund und Kantone erstellen vorsorgliche Planungen zur Bewältigung von schwerwiegenden Ausfällen der kritischen Infrastrukturen.
- *M10:* Die Bevölkerung und die Wirtschaft werden über selbstvorsorgliche Schutzmöglichkeiten für den Fall, dass es zu Ausfällen der kritischen Infrastrukturen kommt, informiert und sensibilisiert.

Kritische Infrastrukturen bei der Ereignisbewältigung unterstützen

Im Falle von akuten Bedrohungen oder bei schwerwiegenden Ausfällen sollen die KI-Betreiber subsidiär mit betriebsexternen Mitteln oder -Fähigkeiten unterstützt werden, um die Bedrohungen abzuwehren, respektive die Gewährleistung eines Minimalbetriebs und die rasche Rückkehr zum Normalbetrieb zu ermöglichen.[5] Als Voraussetzung dafür sind erstens entsprechende Mittel oder Fähigkeiten erforderlich. Währenddem diesbezüglich Einsatzkräfte zur Abwehr von physischen Bedrohungen beigezogen werden können, sind zur Bewältigung von Cyber-Risiken schwerwiegenden Ausmasses nur ungenügende staatliche Mittel (insbesondere nicht ausreichende personelle Ressourcen) vorhanden. Zweitens gilt es, im Falle einer ausserordentlichen Lage die vorhandenen Mittel und die entsprechenden Bedürfnisse zu erfassen (insbesondere in Bezug auf Notstromaggregate und Kommunikationsmittel). Drittens ist sicherzustellen, dass über die Zuteilung der Mittel auf strategischer Ebene unter Berücksichtigung der Bedeutung (Kritikalität) der kritischen Infrastrukturen, der Bedrohungslage und der zur Verfügung stehenden Mittel entschieden werden kann. Viertens sind auch vorgängige Planungen notwendig, um den wirkungsvollen Einsatz der Mittel zu gewährleisten.

Ziel:

- Die Betreiber von kritischen Infrastrukturen werden unter Berücksichtigung ihrer Bedeutung subsidiär mit externen Mitteln wirkungsvoll unterstützt, um Bedrohungen abzuwehren, respektive einen Minimalbetrieb und eine rasche Rückkehr zum Normalbetrieb zu ermöglichen.

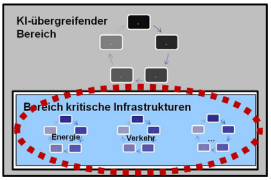
Massnahmen:

- *M11:* Es sind ausreichende staatliche Mittel zur subsidiären Unterstützung der Betreiber kritischer Infrastrukturen bei der Bewältigung von Cyber-Risiken schwerwiegenden Ausmasses zu schaffen.
- *M12:* Im Hinblick auf ausserordentliche Lagen sind die vorhandenen Ressourcen für die Gewährleistung eines Minimalbetriebs und die Rückkehr zum Normalbetrieb zu erfassen.
- *M13:* Die Prozesse betreffend die Zuteilung der externen Mittel zur Unterstützung der Betreiber bei der Ereignisbewältigung sind mit den betroffenen Stellen zu definieren.
- *M14:* Die Zusammenarbeit der Krisen- und Führungsorgane auf den Stufen Bund, Kantone und Gemeinden mit den KI-Betreibern ist zu verstärken, und es sind Einsatzplanungen zum Schutz der national kritischen Infrastruktur-Objekte zu erstellen.

[5] Dabei handelt es sich etwa um Einsatzkräfte (Polizei, Feuerwehr, Zivilschutz, Armee), Kommunikationsmittel oder Notstromaggregate.

7.2 Integralen Schutz im Bereich der kritischen Infrastrukturen verbessern (Handlungsfeld B)

Neben dem KI-übergreifenden Bereich stärkt die nationale SKI-Strategie auch den integralen Schutz im Bereich der kritischen Infrastrukturen.



Da schwerwiegende Ausfälle durch infrastrukturspezifische Risiken verursacht werden können, die entweder ein kritisches Einzelelement (z.B. eine Leitstelle), einen kritischen Teilsektor (z.B. durch ein überaltertes Transportnetz) oder einen kritischen Sektor (z.B. Verkehr) betreffen, soll der integrale Schutz gemäss Ziffer 6 der nationalen SKI-Strategie auf allen relevanten Ebenen der kritischen Infrastrukturen gestärkt werden. Zu diesem Zweck sollen für die kritische Infrastrukturen integrale Schutzkonzepte erarbeitet und umgesetzt werden. Das diesbezügliche Vorgehen wird beispielsweise in einem Leitfaden beschrieben, der gestützt auf die SKI-Grundstrategie des Bundesrates erarbeitet wird. In den integralen Schutzkonzepten werden u.a. laufende oder geplante Arbeiten sowie geltende Rechtsgrundlagen, Schutzziele usw. erfasst und miteinbezogen. Anschliessend werden verbleibende infrastrukturspezifische Risiken ermittelt, Schutzziele festgelegt und gegebenenfalls entsprechende Massnahmen zur Reduktion der Risiken erarbeitet. Weiter wird in den integralen Schutzkonzepten auch geprüft, wie die allfällig notwendigen Schutzmassnahmen finanziert werden können und welche rechtlichen Grundlagen zur Umsetzung der integralen Schutzkonzepte notwendig sind.

Die integralen Schutzkonzepte sollen in Zusammenarbeit mit den jeweils massgebenden Akteuren (zuständige Leitbehörden auf den Stufen Bund, Kantone oder Gemeinden, Betreiber, gefährdungs- oder massnahmenspezifische Fachstellen, Verbände usw.) erarbeitet und umgesetzt werden. Die Verantwortung (insb. bezüglich der Festlegung der Schutzziele) liegt bei den gemäss geltenden Rechtsgrundlagen zuständigen Stellen. Dementsprechend erfolgen die Festlegung der Schutzziele und der Finanzierung von allfällig zusätzlich notwendigen Schutzmassnahmen im Rahmen der teilsektorspezifischen Politikbereiche. Die Arbeiten orientieren sich dabei an einem risikobasierten Kosten-Wirksamkeits-Ansatz: Dies bedeutet, dass nur Massnahmen getroffen werden, welche zur Erfüllung der Schutzziele notwendig sind, respektive bezüglich ihrer Kosten in einem positiven Verhältnis zu ihrem Nutzen stehen. Die integralen Schutzkonzepte sollen dementsprechend vor allem dazu dienen, eine umfassende Sicht über relevante Risiken und Verletzlichkeiten zu erhalten, das bestehende Schutzniveau zu prüfen sowie allfällige Lücken zu identifizieren und zu schliessen.

Ziel:

- Der integrale Schutz der kritischen Infrastrukturen ist auf allen relevanten Ebenen (kritische Sektoren, kritische Teilsektoren und kritische Einzelelemente) gewährleistet. Alle relevanten Risiken sind erkannt und gestützt auf Schutz- und Leistungszielen, die auf politischer Ebene vereinbart wurden, nach einem risikobasierten Kosten-Wirksamkeits-Ansatz reduziert. Dabei wird ein umfassendes Gefahren- und Massnahmenspektrum berücksichtig.

Massnahme:

– *M15:* Es sind, z.B. gestützt auf den SKI-Leitfaden, integrale Schutzkonzepte für die kritischen Infrastrukturen zu erarbeiten und auf Basis einer entsprechenden Rechtsgrundlage umzusetzen. Die integralen Schutzkonzepte werden in Zusammenarbeit mit allen jeweils relevanten Akteuren (Leit- und Fachbehörden auf Stufen Bund, Kantone und Gemeinden, Betreiber, Verbände usw.) erarbeitet und umgesetzt. Die in Tabelle 2 genannten Stellen legen fest, welche Stellen jeweils federführend und mit einzubeziehen sind.

8 Umsetzung der nationalen SKI-Strategie

8.1 Strukturen und Zuständigkeiten

Die Umsetzung der nationalen SKI-Strategie erfolgt massgeblich im Rahmen der etablierten Prozesse und innerhalb der bestehenden Strukturen und Zuständigkeiten. Die Koordination wird durch den frühzeitigen Einbezug der relevanten Behörden (auf Stufen Bund und Kantone), der Wirtschaft (insbesondere Betreiber kritischer Infrastrukturen) und der Wissenschaft sichergestellt. Dabei wird unter anderem auch die Zusammenarbeit mit dem Konsultations- und Koordinationsmechanismus Sicherheitsverbund Schweiz (KKM SVS) gewährleistet.

Die Koordinationsstelle SKI unterstützt die zuständigen Stellen bei der Umsetzung der verschiedenen Massnahmen. Sie ist insbesondere für folgende Aufgaben verantwortlich:

– Koordination der Massnahmen gemäss integralem Schutzprozess im KI-übergreifenden Bereich (Führung des SKI-Inventars usw.)

– Unterstützung der verantwortlichen Behörden und Betreiber bei der Erarbeitung von integralen Schutzkonzepten im Bereich der kritischen Infrastrukturen

– Beratung der Kantone bei SKI-relevanten Arbeiten

– Vorbereitung der Geschäfte für die Koordinationsplattformen

– Kontaktstelle für SKI-relevante Aspekte im internationalen Umfeld

– Berichterstattung über den Stand der Umsetzung der nationalen SKI-Strategie

Eine zentrale Aufgabe stellt weiter die Koordination mit ähnlich gelagerten Arbeiten dar (u.a. nationale Strategie zum Schutz vor Cyber-Risiken, Strategie Zukunft nationale Infrastrukturnetze, Risikomanagement Bund, Wirtschaftliche Landesversorgung). Dieser wird zum einen sichergestellt, indem im KI-übergreifenden Bereich ein Abgleich hinsichtlich methodisches Vorgehen und Erkenntnisse erfolgt. Zum andern werden im Bereich der einzelnen kritischen Infrastrukturen auch die entsprechende Resultate aus diesen Arbeiten im Rahmen der integralen Schutzkonzepte berücksichtigt.

Zuständig für die Umsetzung der Massnahmen im KI-übergreifenden Bereich (M1–M14) sind die im Anhang bezeichneten Stellen. Die Koordinationsstelle SKI übernimmt im KI-übergreifenden Bereich im Rahmen ihrer Prozessverantwortung eine Koordinationsfunktion. Sie prüft gemeinsam mit den genannten Stellen, welche

bestehenden Projekte, Prozesse usw. im Kontext der jeweiligen Massnahme relevant sind, inwiefern die in der Strategie formulierten Ziele dadurch bereits erfüllt werden und welcher zusätzliche Handlungsbedarf besteht. Nach Möglichkeit werden die Massnahmen im Rahmen der laufenden Projekte oder Tätigkeiten umgesetzt.

Ein analoges Vorgehen kommt auch im Bereich der kritischen Infrastrukturen (M15) zum Tragen, wo die die Prozessverantwortung bei den jeweils gemäss geltenden Rechtsgrundlagen zuständigen Behörden (Bund, Kantone oder Gemeinden) liegt. Die in Tabelle 2 festgehaltenen Stellen sind aufgefordert, gegebenenfalls in Zusammenarbeit mit der Koordinationsstelle SKI festzulegen, welche Stellen bei der Erarbeitung federführend und mit einzubeziehen sind. Die Erarbeitung der integralen Schutzkonzepte erfolgt in Zusammenarbeit mit allen jeweils relevanten Akteuren (Betreiber, Verbände, gefährdungs- und massnahmenspezifische Fachstellen usw.). Bei Bedarf und nach Möglichkeiten kann die Koordinationsstelle SKI die Arbeiten begleiten.

Tabelle 2

Teilsektor-spezifische Zuständigkeiten

Sektor	Teilsektor (KTS)	koordinierende Bundesstellen (*nicht abschliessend*)*
Behörden	Diplomatische Vertretungen und Sitze internationaler Organisationen	EDA, fedpol
	Forschung und Lehre	SBF
	Kulturgüter	BABS, BAK
	Parlament, Regierung, Justiz, Verwaltung	BK, Parlamentsdienste, fedpol, BBL, ISB und LE
Energie	Erdgasversorgung	BFE, BWL, ERI
	Erdölversorgung	BFE, BWL, ERI
	Stromversorgung	BFE, BWL, ElCom, ENSI, ESTI
Entsorgung	Abfälle	BAFU
	Abwasser	BAFU
Finanzen	Banken	FINMA, SNB, EFV, SIF
	Versicherungen	FINMA, BSV
Gesundheit	Ärztliche Betreuung und Spitäler	KSD
	Labors	BAG
Industrie	Chemie- und Heilmittelindustrie	BWL
	Maschinen-, Elektro- und Metallindustrie	BWL
Information und Kommunikation	Informationstechnologien	BWL, ISB
	Medien	BAKOM
	Postverkehr	GS UVEK, BAKOM
	Telekommunikation	BAKOM, BWL
Nahrung	Lebensmittelversorgung	BWL, BLW
	Wasserversorgung	BAFU, BWL
Öffentliche Sicherheit	Armee	IOS
	Blaulichtorganisationen	BABS, fedpol, NDB
	Zivilschutz	BABS
Verkehr	Luftverkehr	BAZL, BWL
	Schienenverkehr	BAV, BWL
	Schiffsverkehr	BAV, BWL
	Strassenverkehr	ASTRA, BWL

* Die genannten Stellen nehmen eine koordinierende Rolle ein: Bei Bedarf legen sie gemeinsam mit der Koordinationsstelle SKI fest, welche Stellen (Bund, Kantone, Verbände usw.) bei der Erarbeitung der integralen Schutzkonzepte federführend und mit einzubeziehen sind. Geltende Kompetenzen bleiben vorbehalten.

8.2 Zeitplan und Controlling

Die Umsetzung der einzelnen Massnahmen wird mit Hilfe eines detaillierten Umsetzungs- und Controlling-Plans konkretisiert, der nach Verabschiedung der nationalen SKI-Strategie erarbeitet wird. In groben Zügen soll die Umsetzung in folgendem Zeitplan erfolgen:

Phase 1 (bis Ende 2012)

- Die Umsetzungsplanung ist erstellt.
- Die auf nationaler Ebene kritischen Infrastruktur-Objekte sind identifiziert und erfasst. (M1)
- Die sektorübergreifenden Plattformen (AG SKI und AG Betreiber) sind eingerichtet. (M3)

Phase 2 (bis Ende 2013)

- Das Konzept zur Sicherstellung der Warnung im Ereignisfall ist fertig gestellt. (M5)
- Grundlagen und Anträge für auf einander abgestimmte Schutzziele liegen vor. (M6)
- Eine Vorlage zu einer Rechtsgrundlage zur Sicherheitsüberprüfung von Betreibern kritischer Infrastrukturen ist vorhanden. (M7)
- Bestehende Abschalt- und Bewirtschaftungspläne sind mit national kritischen Infrastrukturen ergänzt. (M8)
- Ein Mechanismus zur Erfassung bestehender Ressourcen ist entwickelt. Die Prozesse zur Unterstützung von Betreibern mit externen Mitteln sind definiert. (M12, M13)

Phase 3 (bis Ende 2014)

- Ein aktualisierter Vorschlag für ein nationales Forschungsprogramm ist eingereicht. Weitere Abklärungen auf der Ebene Ressortforschung sind erfolgt. (M2)
- Ergebnisse zur Überprüfung der Befugnisse und Kapazitäten bei der Überwachung der Gefährdungen liegen vor. (M4)
- Informationsprodukte zur Stärkung der Selbstvorsorge von Wirtschaft und Bevölkerung sind erstellt. (M10)
- Einsatzplanungen zum physischen Schutz der kritischen Infrastrukturen sind erarbeitet. (M14)

Phase 4 (ab 2015)

- Vorsorgliche Planungen zur Bewältigung von Ausfällen kritischer Infrastrukturen sind erarbeitet. (M9)
- Die personellen Ressourcen und Fähigkeiten für die subsidiäre Unterstützung zur Bewältigung von Cyber-Risiken werden basierend auf entsprechenden Rechtsgrundlagen gestaffelt geschaffen. (M11)

– Integrale Schutzkonzepte für die kritischen Infrastrukturen sind erarbeitet und werden umgesetzt. (M15)

Dem Bundesrat wird alle vier Jahre über den Stand der Umsetzung Bericht erstattet.

8.3 Revision der SKI-Strategie

Die nationale Strategie zum Schutz kritischer Infrastrukturen wird periodisch aktualisiert. Die vorliegende Strategie wird überprüft und gegebenenfalls bis Ende 2016 angepasst.

Massnahmen und Nahtstellen mit laufenden oder geplanten Arbeiten

Massnahme	Zuständige Stellen (*nicht abschliessend*)*	Nahtstellen mit anderen Projekten/Stellen/Organisationen (*nicht abschliessend*)
M1: Erstellung SKI-Inventar	BABS, Bundesstellen gemäss Tabelle 2, Kantone (Kantonale Kontaktstellen SKI)	Bestehende Verzeichnisse/Inventare (Störfallkataster, Stauanlagen, Kulturgüter usw.)
M2: Lancierung Forschungsprogramme (inkl. nationales Forschungsprogramm)	BABS	Schweizerischer Nationalfonds SNF, Forschungsprogramme der Bundesstellen
M3: Einrichtung Plattformen Behörden/ Fachstellen und Betreiber	BABS	Wirtschaftliche Landesversorgung (WL), Nachrichtendienst des Bundes (NDB), Nationale Strategie zum Schutz vor Cyber-Risiken
M4: Überprüfung Befugnisse und Kapazitäten zur Überwachung der Gefährdungen	BAFU, BWL, MeteoSchweiz, NDB	Gemeinsame Informationsplattform Naturgefahren (GIN), Erarbeitung Nachrichtendienstgesetz, Melde- und Analysestelle Informationssicherung MELANI, WL, Strategie Cyber-Risiken
M5: Etablierung Mechanismus Frühwarnung	BABS, BAFU, BWL, MeteoSchweiz, NDB	Projekt Netalert (BABS), Melde- und Analysestelle Informationssicherung MELANI, WL
M6: Erarbeitung von übergeordneten Schutzzielen	BABS	Interdepartementale Plattform Naturgefahren PLANAT, WL
M7: Schaffung gesetzliche Grundlage zur Sicherheitsüberprüfung von KI-Betreibern	IOS	Projekt formell-gesetzliche Grundlage für den Informationsschutz (FOGIS), Informations- und Objektsicherheit IOS

Massnahme	Zuständige Stellen (*nicht abschliessend*)*	Nahtstellen mit anderen Projekten/Stellen/Organisationen (*nicht abschliessend*)
M8: Überarbeitung bestehender Abschalt- und Bewirtschaftungspläne	BWL	BFE, ELCOM
M9: Erarbeitung von vorsorglichen Planungen im Hinblick auf KI-Ausfälle	BABS, Kantone (Kantonale Führungsorgane KFO), BWL, BFE	Bundesstab ABCN (BST ABCN), Kantonale Gefährdungsanalysen (KATAPLAN), WL, IDA Nomex
M10: Verbesserung Selbstvorsorge von Wirtschaft und Bevölkerung	BABS, BWL, BK	Projekt individuelle Schutzmassnahmen (BABS), BK
M11: Gewährleistung subsidiäre Unterstützung bei Bewältigung von Cyber-Risiken	NDB, ISB, BWL	Nationale Strategie zum Schutz vor Cyber-Risiken
M12: Erfassung von Ressourcen zum Notbetrieb von kritischen Infrastrukturen	BABS	Ressourcenmanagement Bund (ResMaB), WL
M13: Festlegung Prozesse zur Zuteilung von externen Mitteln an KI-Betreiber	BABS	Sicherheitsverbund Schweiz (SVS), BST ABCN, ResMaB, WL, IDA Nomex
M14: Verstärkung Zusammenarbeit Führungsorgane – KI-Betreiber und Erarbeitung Schutzplanungen	BST ABCN, Kantone, Gemeinden (Führungsorgane, Polizei, Feuerwehr), FST A	SVS, Weiterentwicklung Bevölkerungsschutz/ Zivilschutz, KATAPLAN, IDA Nomex

Massnahme	Zuständige Stellen (*nicht abschliessend*)*	Nahtstellen mit anderen Projekten/Stellen/Organisationen (*nicht abschliessend*)
M15: Erarbeitung und Umsetzung von integralen Schutzkonzepten für kritische Infrastrukturen	Nach Absprache mit koordinierenden Stellen gemäss Tabelle 2	Diverse sektor- und gefährdungsspezifische Arbeiten (u.a. Strategie Informationsgesellschaft Schweiz, Strategie Cyber-Risiken, Erdbebenvorsorge, Risikomanagement Bund, Priorisierung Bundesgebäude bei Stromausfall)

* Die Koordinationsstelle SKI übernimmt jeweils eine Koordinationsfunktion und stellt mit den genannten Stellen den Einbezug aller zuständigen und relevanten Stellen sicher.